

REMARKS

Reconsideration of this application is respectfully requested.

In response to the rejection of claims 19-21 and 27 under 35 U.S.C. 112, second paragraph, claims 19, 20 and 27 have been cancelled above without prejudice or disclaimer thereby mooting this ground of rejection with respect to those claims. Claim 21 has been amended so as to claim the data storage medium rather than mere abstract "data" -- thus now claiming a physical entity.

Accordingly, all outstanding formal issues are now believed to have been resolved in the applicant's favor.

The rejection of claims 1-27 under 35 U.S.C. §103 as allegedly "obvious" over a four-way combination of Yourdon, Dean, Wobber '642 and Richardson '204 is respectfully traversed.

The Examiner admits that Yourdon and Dean et al "do not directly address this specific program of protecting from copying data, and authentication which have been downloaded from a server to a client, nor its solution as in claim 1". In an apparent attempt to supply these admitted deficiencies, the Examiner then briefly discusses Wobber with respect to authentication issues. Although the Examiner does not expressly admit that this three-way combination of references still has admitted deficiencies, the Examiner introduces the next paragraph with the word "nevertheless":

"Nevertheless it is held that one with skills in the art would need no inventive activity to infer from the general teachings of Yourdon ('to determine the end user's authorization to invoke certain functionalities of access certain data'", and Dean et al 'applets can name only those functions in variables explicitly exported to the Java sub-system"', at least when taken in combination, that a solution consists in selectively controlling copying functions of the client in respect of the downloaded data, hence arriving at the subject matter of claim 1." [last paragraph on page 6].

Simply stated, there is no basis in any of three references for the conclusions reached by the Examiner in this "Nevertheless" paragraph.

It is also noted that the Examiner does not provide any supporting argument whatsoever with respect to claims 2-4 and 18-27 (including independent claim 22).

The amended claim 1 includes implementations of the invention where the program portion is not necessarily first downloaded to the client, but is already part of the functionality of the client, for example where the client is a dedicated set-top-box for use with a TV, or where it is a dedicated multimedia audio/video player.

None of the cited prior art appear to disclose using a program portion being run at a client to request access to data and controlling the client to restrict access to copying or saving functions in respect of the data when not cryptographically protected.

Yourdon, on page 28 under the heading "Security", mentions the obvious desire to create application programs that provide secure access to functionality and data, particularly over the Internet. However, he doesn't attempt to describe methods by which

this desire might be satisfied other than through interaction with a web browser to encrypt/decrypt transmissions between a user's workstation and a server.

Dean is concerned solely with flaws in the implementation of Java and the extent to which hackers might use Java applets to gain access to features and data of a user's environment, to cause potential damage to that environment or gain unauthorised access to hosts or data via that environment.

Rather than discuss ways in which Java applets might be used positively to achieve secure access to functionality and data in a particular application, Dean et al disclose only methods by which security features in the Java subsystem might be compromised, in a negative way, by rogue applets. These two aspects are mutually exclusive. In particular, Dean mentions that Java subsystems must be able to limit the access that applets have to functions and variables and other system resources (at a client) in order to be secure. But in the present invention, it is the program portion (e.g., a Java applet) that is being used to restrict access to functions that would otherwise be legitimately available at the client (e.g., provided via the Java subsystem). Dean does not teach how to use legitimately provided Java features, only how to exploit a miscellany of loop-holes that were not intended to be available.

The teaching of Dean et al is of use only in showing how the positive desires of Yourdon -- to provide secure access to functionality and data -- may be compromised, representing a step away from the present invention.

In addition, contrary to the Examiner's assertions regarding Dean et al, there appears to be no disclosure whatsoever regarding use of encryption with Java.

Wobber et al is concerned with the problem of authenticating the source of requests for access to data in a distributed information system. Security of access to data sets at servers within the system is achieved using normal access control lists at the servers to determine who may access particular data sets. Wobber discloses using prior art encryption mechanisms for securing transmission of requested data from host to host once access has been granted.

However, Wobber et al does not appear to disclose any features that restrict what the requestor may do with data once access has been granted and data transferred. Wobber is happy that the data has been supplied to a requestor of known identity with permission to access the data. Wobber therefore offers no teaching towards restricting access by the requestor to copy/save functions in respect of the data at a receiving node.

Richardson is only briefly discussed with respect to claims 5, 6 and 17 -- and even there only collectively discussed with Yourdon and Wobber presumably indicating that Richardson is merely cumulative prior art. However, it is noted that Richardson at page 15, lines 16-20 does disclose using information from a local computer environment as the first stage in generating a security key for registration purposes.

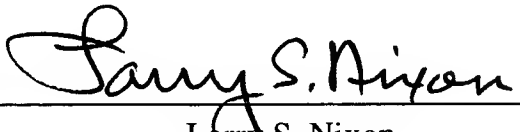
The Examiner's brief discussion of Gosling and Bender et al appears to be an afterthought in addition to the actually stated allegation of "obviousness" based upon four earlier identified references. Nevertheless, if Gosling is merely cited to substantiate that downloading of a program per se is "well known in the art" and Bender et al is merely cited so as to document the fact that steganographical marking of data per se is also "well known in the art", then those points are conceded. However, under 35 U.S.C. §103, the claimed subject matter must be considered "as a whole" -- and not in piecemeal fashion. It often is the case that individual incremental aspects of almost any invention are "well known in the art". It is the inventive act that recognizes and creates novel non-obvious combinations of such previously known building blocks.

Attention is also drawn to new claims 28-30. New independent claim 28 is drawn to a server for providing access to data sets in a protected form. Claim 29 is directed to a computer program carrier medium containing a computer program which implements the functions of the server in claim 28 when installed and run on a server. Claim 30 is an independent method claim for protecting data downloaded from a server computer to a client computer where the downloaded data is a protected copy of requested and where a program is run at the client to both unprotect downloaded data and suppress client computer copy and save functions with respect to the unprotected version of the protected data. The cited prior art is not believed to teach or suggest such inventions.

Accordingly, this entire application is now believed to be in allowable form and a formal Notice to that effect is respectfully submitted.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 
Larry S. Nixon
Reg. No. 25,640

LSN:vc
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703) 816-4000
Facsimile: (703) 816-4100